

THE CRITICAL NUMBER OF DENSE TRIANGLE-FREE BINARY MATROIDS

JIM GEELEN AND PETER NELSON

ABSTRACT. We show that, for each real number $\varepsilon > 0$ there is an integer c such that, if M is a simple triangle-free binary matroid with $|M| \geq (\frac{1}{4} + \varepsilon) 2^{r(M)}$, then M has critical number at most c . We also give a construction showing that no such result holds when replacing $\frac{1}{4} + \varepsilon$ with $\frac{1}{4} - \varepsilon$ in this statement. This shows that the “critical threshold” for the triangle is $\frac{1}{4}$. We extend the notion of critical threshold to every simple binary matroid N and conjecture that, if N has critical number $c \geq 3$, then N has critical threshold $1 - i \cdot 2^{-c}$ for some $i \in \{2, 3, 4\}$. We give some support for the conjecture by establishing lower bounds.

1. INTRODUCTION

If M is a simple binary matroid, viewed as a restriction of a rank- r projective geometry $G \cong \text{PG}(r-1, 2)$, then the *critical number* of M , denoted $\chi(M)$, is the minimum nonnegative integer c such that G has a rank- $(r-c)$ flat disjoint from $E(M)$. A matroid with no $U_{2,3}$ -restriction is *triangle-free*. Our first two main theorems are the following:

Theorem 1.1. *For each $\varepsilon > 0$ there exists $c \in \mathbb{Z}$ such that every simple triangle-free binary matroid M with $|M| \geq (\frac{1}{4} + \varepsilon) 2^{r(M)}$ satisfies $\chi(M) \leq c$.*

Theorem 1.2. *For each $\varepsilon > 0$ and each integer $c \geq 1$, there is a simple triangle-free binary matroid M such that $|M| \geq (\frac{1}{4} - \varepsilon) 2^{r(M)}$ and M has critical number c .*

That is, simple triangle-free binary matroids with density slightly more than $\frac{1}{4}$ have bounded critical number, and those with density slightly less than $\frac{1}{4}$ can have arbitrarily large critical number. Theorem 1.2 refutes an earlier conjecture of the authors [13]. As in [13], the

Date: April 18, 2016.

1991 Mathematics Subject Classification. 05B35.

Key words and phrases. matroids, regularity.

This research was partially supported by a grant from the Office of Naval Research [N00014-10-1-0851].

proof of Theorem 1.1 depends on a regularity lemma due to Green [11]; this material is discussed in Section 2.

The critical number was originally defined by Crapo and Rota [4] under the name of *critical exponent*; our terminology follows Welsh [20]. One can also define $\chi(M)$ as the minimum c so that $E(M)$ is contained in a matroid whose ground set is the union of c affine geometries. In particular, if M is the cycle matroid of a graph G , then $\chi(M)$ is the minimum number of cuts required to cover $E(G)$, so $\chi(M) = 1$ precisely when G is bipartite, and $\chi(M) = \lceil \log_2(\chi(G)) \rceil$ in general. Thus, we can view critical number as a geometric analog of chromatic number; results in graph theory motivate much of the material in this paper.

In analogy to our two main theorems, Hajnal (see [6]) gave examples of triangle-free graphs G with minimum degree $\delta(G) \geq (\frac{1}{3} - \varepsilon) |V(G)|$ and arbitrarily large chromatic number, and Thomassen [19] showed for each $\varepsilon > 0$ that every triangle-free graph G with $\delta(G) \geq (\frac{1}{3} + \varepsilon) |V(G)|$ has chromatic number bounded above by a function of ε .

In fact, something much stronger holds; in [3], Brandt and Thomassé showed that if G is a triangle-free graph G with minimum degree $\delta(G) > \frac{1}{3}|V(G)|$, then $\chi(G) \in \{2, 3, 4\}$. The bound $\chi(G) \leq 4$ is best possible; Häggkvist [14] found an example of a 10-regular triangle-free graph on 29 vertices with chromatic number 4. We conjecture a similar strengthening of Theorem 1.1.

Conjecture 1.3. *If M is a simple triangle-free binary matroid with $|M| > \frac{1}{4}2^{r(M)}$, then $\chi(M) \in \{1, 2\}$.*

Chromatic threshold. Erdős and Simonovits [6] proposed the problem, for a given simple graph H and $\alpha > 0$, of determining the maximum of $\chi(G)$ among all H -free graphs G with minimum degree at least $\alpha|V(G)|$. Extending on this idea, Łuczak and Thomassé [16] define the *chromatic threshold* for H to be the infimum of all $\alpha > 0$ such that there exists $c = c(H, \alpha)$ for which every graph G with no H -subgraph and with minimum degree at least $\alpha|V(G)|$ has chromatic number at most c .

The aforementioned results for the triangle C_3 give that its chromatic threshold is $\frac{1}{3}$. The Erdős-Stone Theorem [7] implies that the chromatic threshold for any bipartite graph H is 0, since large dense H -free graphs do not exist. Quite remarkably, the chromatic thresholds of all graphs have been explicitly determined by Allen et al. in [1]; here we will state a simplified version of their result that limits the threshold to one of three particular values depending only on $\chi(H)$.

Theorem 1.4. *If H is a graph of chromatic number $c \geq 3$, then H has chromatic threshold in $\{\frac{c-3}{c-2}, \frac{2c-5}{2c-3}, \frac{c-2}{c-1}\}$.*

Critical threshold. For a simple binary matroid N , we define the *critical threshold* of N to be the infimum of all $\alpha > 0$ such that there exists $c = c(N, \alpha)$ for which every simple binary matroid M with no N -restriction and with $|M| \geq \alpha 2^{r(M)}$ satisfies $\chi(M) \leq c$. For each integer $k \geq 3$, let C_k denote the k -element circuit $U_{k-1,k}$. Theorems 1.1 and 1.2 imply that the critical threshold for C_3 is $\frac{1}{4}$. In contrast, the main result of [13] shows that, if $k \geq 5$ is odd, then C_k has critical threshold 0.

A result of Bonin and Qin [2], itself a special case of the geometric density Hales-Jewett theorem [8], implies that each simple binary matroid with critical number 1 has critical threshold 0. More generally, the geometric Erdős-Stone theorem [12] gives the following upper bound on the critical threshold of any simple binary matroid.

Theorem 1.5. *The critical threshold for a simple binary matroid N is at most $1 - 2^{1-\chi(N)}$.*

We show, in fact, that this holds with equality fairly often.

Theorem 1.6. *If N is a simple binary matroid of critical number $c \geq 1$ so that $\chi(N \setminus I) = c$ for every rank- $(n - c + 1)$ independent set I of N , then the critical threshold for N is $1 - 2^{1-c}$.*

In Conjectures 5.1 and 5.2, we predict the precise value of the critical threshold for any simple binary matroid. The following is a simplification of those conjectures in the vein of Theorem 1.4.

Conjecture 1.7. *If N is a simple nonempty binary matroid, then the critical threshold for N is equal to $1 - i \cdot 2^{-\chi(N)}$ for some $i \in \{2, 3, 4\}$.*

Specialised to projective geometries, our conjectures give:

Conjecture 1.8. *For each $t \geq 2$, the critical threshold for $\text{PG}(t-1, 2)$ is $1 - 3 \cdot 2^{-t}$.*

Finally, we pose the following strengthening of Conjectures 1.3 and 1.8; the analogous result was proved for graphs by Goddard and Lyle in [9].

Conjecture 1.9. *If $t \geq 2$ and N is a simple binary matroid with no $\text{PG}(t-1, 2)$ -restriction such that $|N| > (1 - 3 \cdot 2^{-t})2^{r(N)}$, then $\chi(N) \in \{t-1, t\}$.*

2. REGULARITY

Green used Fourier-analytic techniques to prove his regularity lemma for abelian groups and to derive applications in additive combinatorics;

these techniques are discussed in greater detail in the book of Tao and Vu [18, Chapter 4]. Fortunately, although this theory has many technicalities, the group $\text{GF}(2)^n$ is among its simplest applications.

Let $V = \text{GF}(2)^n$ and let $X \subseteq V$. Note that, if H is a 1-codimensional subspace of V , then $|H| = |V \setminus H|$. We say that X is ε -uniform if for each 1-codimensional subspace H of V we have

$$||H \cap X| - |X \setminus H|| \leq \varepsilon|V|.$$

In Lemma 2.2 we will see that, for small ε , the ε -uniform sets are ‘pseudorandom’.

Let H be a subspace of V . For each $v \in V$, let $H_v(X) = \{h \in H : h + v \in X\}$. For $\varepsilon > 0$, we say H is ε -regular with respect to V and X if $H_v(X)$ is ε -uniform in H for all but $\varepsilon|V|$ values of $v \in V$.

Regularity captures the way that X is distributed among the cosets of H in V . For $v \in V$, we let $X + v = \{x + v : x \in X\}$; thus $X + v$ is a translation of X . Note that $X + v$ is ε -uniform if and only if X is. Also note that $H_v(X) + v = X \cap H'$ where $H' = H + v$ is the coset of H in V that contains v . Therefore, if $u, v \in H'$, then $H_u(X)$ and $H_v(X)$ are translates of one another. So H is ε -regular if, for all but an ε -fraction of cosets H' of H , the set $(H' \cap X) + v$ is ε -uniform in H for some $v \in H'$.

The following result of Green [11] guarantees a regular subspace of bounded codimension. Here $T(\alpha)$ denotes an exponential tower of 2’s of height $\lceil \alpha \rceil$.

Lemma 2.1 (Green’s regularity lemma). *Let X be a set of points in a vector space V over $\text{GF}(2)$ and let $0 < \varepsilon < \frac{1}{2}$. Then there is a subspace H of V , having codimension at most $T(\varepsilon^{-3})$, that is ε -regular with respect to X and V .*

If A_1, A_2, A_3 were random subsets of $\text{GF}(2)^n$ with $|A_i| = \alpha_i 2^n$, we would expect approximately $\alpha_1 \alpha_2 \alpha_3 2^{2n}$ solutions to the linear equation $a_1 + a_2 + a_3 = 0$ with $a_i \in A_i$. The next lemma, found in [11] and also a corollary of [18, Lemma 4.13], bounds the error in such an estimate when at least two of these sets are uniform.

Lemma 2.2. *Let V be an n -dimensional vector space over $\text{GF}(2)$, and let $A_1, A_2, A_3 \subseteq V$ with $|A_i| = \alpha_i |V|$. If $0 < \varepsilon < \frac{1}{2}$ and A_1 and A_2 are ε -uniform, then*

$$|\{(a_1, a_2, a_3) \in A_1 \times A_2 \times A_3 : a_1 + a_2 + a_3 = 0\}| \geq (\alpha_1 \alpha_2 \alpha_3 - \varepsilon) 2^{2n}.$$

3. TRIANGLE-FREE BINARY MATROIDS

We mostly use standard notation from matroid theory [17]. It will also be convenient to think of a simple rank- n binary matroid as a subset of the vector space $V = \text{GF}(2)^n$. For $X \subseteq V - \{0\}$, we write $M(X)$ for the simple binary matroid on X represented by a binary matrix with column set X .

We require an easy lemma about triples of vectors with sum zero.

Lemma 3.1. *If X is a set of elements in an n -dimensional vector space V over $\text{GF}(2)$ with $|X| > 2^{n-1}$, then for all $v \in V$ there exist $x_1, x_2 \in X$ such that $x_1 + x_2 + v = 0$.*

Proof. If $v = 0$, the result is trivial. If $v \neq 0$, the elements of V partition into 2^{n-1} pairs (x, y) with $x + y + v = 0$. Since $|X| > 2^{n-1}$, some such pair contains two elements of X , giving the result. \square

We now prove Theorem 1.1 by means of the following stronger result, which shows that the theorem holds not just for triangle-free matroids but for all matroids in which each element is in $o(2^r)$ triangles.

Theorem 3.2. *For each $\varepsilon > 0$ there exist $c \in \mathbb{Z}$ and $\beta > 0$ such that, if M is a simple binary matroid with $|M| \geq (\frac{1}{4} + \varepsilon)2^{r(M)}$, then either $\chi(M) \leq c$, or there is some $e \in E(M)$ contained in at least $\beta 2^{r(M)}$ triangles of M .*

Proof. We may assume that $\varepsilon < \frac{3}{4}$. Let $\delta = \frac{1}{16}\varepsilon^3$, noting that $\delta < \frac{1}{2}$ and $(1 + 2\delta)^2 < 1 + 2\varepsilon$, and set $c \geq T(\delta^{-3})$. Let $\beta = 2^{-2c}\delta$.

Let M be a simple rank- r binary matroid with $|M| \geq (\frac{1}{4} + \varepsilon)2^{r(M)}$. Let $V = \text{GF}(2)^r$ and $X \subseteq V$ be such that $M = M(X)$. Suppose that each $e \in E(M)$ lies in at most $\beta 2^{r(M)}$ triangles of M .

Since $\delta < \frac{1}{2}$, by Lemma 2.1 there is a subspace H of V that is δ -regular with respect to X and V and has codimension $k \leq c$ in V . If $X \cap H = \emptyset$ then $\chi(M) \leq k \leq c$, giving the theorem, so we may assume that there is some $v_0 \in X \cap H$. Let W be the subspace of V that is ‘orthogonal’ to H ; thus $|W| = 2^k$ and $\{H + w : w \in W\}$ is the collection of cosets of H in V . We first claim that X is not too dense in any coset:

Claim 3.2.1. $|X \cap (H + w)| \leq (\frac{1}{2} + \delta)2^{r-k}$ for each $w \in W$.

Proof of claim: The elements of $H + w$ partition into 2^{r-k-1} pairs adding to v_0 ; since the element of M corresponding to v_0 is in at most $\beta 2^r$ triangles of M , at most $\beta 2^r$ of these pairs contain two elements of X . (This also holds for $w = 0$ since $0 \notin X$.) Therefore

$$|(H + w) \cap X| \leq 2^{r-k-1} + \beta 2^r \leq (\frac{1}{2} + 2^k \beta) 2^{r-k} \leq (\frac{1}{2} + \delta) 2^{r-k},$$

as required. \square

Let $Z = \{w \in W : |X \cap (H + w)| \geq \frac{\varepsilon}{2} 2^{r-k}\}$.

Claim 3.2.2. $|Z| > (\frac{1}{2} + \delta) 2^k$.

Proof of claim: Using the first claim and $|W \setminus Z| \leq 2^k$, we have

$$\begin{aligned} \left(\frac{1}{4} + \varepsilon\right) 2^r &\leq |X| \\ &= \sum_{w \in W} |X \cap (H + w)| \\ &\leq \sum_{w \in Z} \left(\frac{1}{2} + \delta\right) 2^{r-k} + \sum_{w \in W \setminus Z} \frac{\varepsilon}{2} 2^{r-k} \\ &\leq 2^{r-k} \left(\left(\frac{1}{2} + \delta\right) |Z| + \frac{\varepsilon}{2} 2^k \right). \end{aligned}$$

Thus $|Z| \geq \frac{1+2\varepsilon}{2(1+\delta)} 2^k > (\frac{1}{2} + \delta) 2^k$, where we use $(1+2\delta)^2 < 1+2\varepsilon$. \square

By regularity there are at most $\delta 2^k$ values of $w \in W$ such that $H_w(X)$ is not δ -uniform, so there is a set $Z' \subseteq Z$ such that $|Z'| > 2^{k-1}$ and $H_w(X)$ is δ -uniform for each $w \in Z'$. By Lemma 3.1, there are elements $w_1, w_2, w_3 \in Z'$ such that $w_1 + w_2 + w_3 = 0$. The sets $H_{w_1}(X), H_{w_2}(X), H_{w_3}(X)$ are δ -uniform subsets of H with at least $\frac{1}{2}\varepsilon 2^{r-k}$ elements; by Lemma 2.2 the number of solutions to $x_1 + x_2 + x_3 = 0$, so that $x_i \in H_{w_i}(X)$ for each $i \in \{1, 2, 3\}$, is at least $\left(\left(\frac{1}{2}\varepsilon\right)^3 - \delta\right) 2^{2(r-k)} = \delta 2^{-2k} 2^{2r} \geq \beta 2^{2r}$. For any such solution, the vectors $x_1 + w_1, x_2 + w_2, x_3 + w_3$ are elements of X summing to zero, so M has at least $\beta 2^{2r}$ triangles. It follows, since $|M| < 2^r$, that some $e \in E(M)$ is in more than $\beta 2^r$ triangles, a contradiction. \square

The lower bound. Theorem 1.1 establishes an upper bound of $\frac{1}{4}$ on the critical threshold of C_3 . We have yet to prove Theorem 1.2 which gives the corresponding lower bound. We will in fact prove a stronger result, Theorem 5.4. However, in the generalisation, we lose the simplicity of the construction that works for C_3 , so we give that construction here. The construction is very close to that of a ‘niveau set’ (see [10], Theorem 9.4).

Let $c, n \geq 0$ be integers. Let X_n denote the set of vectors in $\text{GF}(2)^{n+1}$ with first entry zero and Hamming weight greater than $n - c$. Let Y_n denote the set of vectors in $\text{GF}(2)^{n+1}$ with first entry 1 and Hamming weight at most $\frac{1}{2}(n - c)$. Let $M_{c,n}$ denote the matroid $M(X_n \cup Y_n)$. The following lemma implies Theorem 1.2.

Lemma 3.3. *Let $c \geq 0$ be an integer and $\varepsilon > 0$. Then, for each sufficiently large integer n , the matroid $M = M_{c,n}$ is triangle-free, has critical number $c + 1$, and satisfies $|M| \geq (\frac{1}{4} - \varepsilon)2^{r(M)}$.*

Proof. Suppose that $n > 3c$. Clearly $(Y_n + Y_n) \cap X_n$ and $(X_n + X_n) \cap X_n$ are empty; it follows that M is triangle-free. By Stirling's approximation, $\max_{0 \leq i \leq n} \binom{n}{i} \leq \binom{n}{\lfloor n/2 \rfloor} = O(\frac{2^n}{\sqrt{n}}) = o(2^n)$, so

$$|Y_n| = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{i} - \sum_{i=\lfloor (n-c)/2 \rfloor}^{\lfloor n/2 \rfloor} \binom{n}{i} \geq \frac{1}{2}2^n - \frac{c}{2}o(2^n);$$

since $r(M) = n + 1$ and $|M| \geq |Y_n|$, this implies the required lower bound on $|M|$ for sufficiently large n . Let b_1, \dots, b_{n+1} be the standard basis for $\text{GF}(2)^{n+1}$ and let $\mathbf{j} = \sum b_i$. If $W = \text{span}(\{b_2, \dots, b_{n+1-c}\})$, then $\text{codim}(W) = c + 1$ and $W \cap E(M) = \emptyset$, so $\chi(M) \leq c + 1$.

Finally, we show that $\chi(M) > c$. Let U be a subspace of $\text{GF}(2)^{n+1}$ with $\text{codim}(U) \leq c$ and let A be a matrix with at most c rows having null space U . If there is some $y \in U$ with first entry 1, then there exists $x \in \text{GF}(2)^{n+1}$ with first entry zero and Hamming weight at most $\text{rank}(U) \leq c$ such that $Ax = A(y + b_1)$, giving $A(x + b_1) = Ay = 0$. Now $x + b_1$ has first entry 1 and Hamming weight at most $c + 1 < \frac{1}{2}(n - c)$, so $x + b_1 \in U \cap Y_n$ and therefore $U \cap E(M) \neq \emptyset$. Suppose, therefore, that every $y \in U$ has first entry zero. Now there is a vector $z \in \text{GF}(2)^{n+1}$ of Hamming weight at most c such that $Az = A\mathbf{j}$; we have $z + \mathbf{j} \in U$ (and therefore $z + \mathbf{j}$ has first entry zero) and $z + \mathbf{j}$ has Hamming weight at least $n + 1 - c$, so $z + \mathbf{j} \in X_n \cap U$, again giving $U \cap E(M) \neq \emptyset$. This completes the proof. \square

4. LARGE GIRTH AND CRITICAL NUMBER

Jaeger [15] gave a constructive characterisation of matroids with large critical number. Erdős [5] used a probabilistic argument to prove the existence of graphs with large girth and chromatic number, which, since $\chi(M(G)) = \lceil \log_2(\chi(G)) \rceil$ for each graph G , gives binary matroids with large girth and critical number. We will use the probabilistic method to construct such matroids with the additional property that they have a representation comprising only vectors of large support.

For $x \in \text{GF}(2)^S$, let $\text{supp}(x)$ denote the support of x : that is, the set of all $s \in S$ such that $x_s \neq 0$. Let $\text{wt}(x) = |\text{supp}(x)|$ denote the Hamming weight of x . We require the following technical lemma, concerning vectors of small Hamming weight.

Lemma 4.1. *Let $c, s, n \in \mathbb{Z}$ with $n \geq 2^{c+1}s$ and $s > c$, and let W be a $c \times n$ binary matrix. For each $v \in \text{GF}(2)^n$, the number of vectors $x \in \text{GF}(2)^n$ satisfying $Wx = Wv$ and $\text{wt}(x) \leq s$ is at least $\left(\frac{n}{2^{c+1}s}\right)^{s-c-1}$.*

Proof. Let $[n] = \{1, \dots, n\}$ index the column set of W . Since Wv is in the column space of W , there is a vector $v_0 \in \text{GF}(2)^n$ with $\text{wt}(v_0) \leq \text{rank}(W) \leq c$ such that $Wv_0 = Wv$; let $I = \text{supp}(v_0) \subseteq [n]$. The matrix W has at most 2^c distinct columns, so there is a set $J \subseteq [n] - I$ and a vector $w_0 \in \text{GF}(2)^c$ such that $W_j = w_0$ for each $j \in J$ and

$$|J| \geq 2^{-c}([n] - |I|) \geq 2^{-c}(n - c) \geq 2^{-c-1}n \geq s.$$

If $s - |I|$ is even, then each vector x such that $\text{wt}(x) = s$ and $I \subseteq \text{supp}(x) \subseteq I \cup J$ satisfies $Wx = Wv_0 + (s - |I|)w_0 = Wv$. If $s - |I|$ is odd, then each vector x such that $\text{wt}(x) = s - 1$ and $I \subseteq \text{supp}(x) \subseteq I \cup J$ satisfies $Wx = Wv_0 + (s - |I| - 1)w_0 = Wv$. The number of vectors x with $\text{wt}(x) \leq s$ and $Wx = Wv$ is therefore at least

$$\min \left(\binom{|J|}{s - |I|}, \binom{|J|}{s - 1 - |I|} \right) \geq \left(\frac{|J|}{s} \right)^{s - |I| - 1} \geq \left(\frac{n}{2^{c+1}s} \right)^{s - c - 1},$$

as required. \square

The following lemma gives a subset of $\text{GF}(2)^n$ of high girth and critical number, such that every vector has very large Hamming weight.

Lemma 4.2. *For all integers $c, g \geq 2$ and all sufficiently large $n \in \mathbb{Z}$, there is a set $Z \subseteq \text{GF}(2)^n$ such that $M(Z)$ has girth at least g and critical number at least c , and $\text{wt}(z) \geq n - 2cg$ for each $z \in Z$.*

Proof. Let $s = 2cg$ and let $\mu = 2^{c(c-s)}s^c$. Let n be a sufficiently large integer such that $n \geq s$ and $(2s^s)^{-1/g}n^{2c} \geq c\mu^{-1}n^{c+1} + 1$. We show that the result holds for n .

Let S be the set of vectors in $\text{GF}(2)^n$ of Hamming weight at least $n - s$ and let $m = \left\lfloor \left(\frac{1}{2}|S|\right)^{1/g} \right\rfloor$. Using $|S| \geq \left(\frac{n}{s}\right)^s$ and our choice of n , we have

$$m \geq \left(\frac{1}{2s^s}\right)^{1/g}n^{s/g} - 1 = (2s^s)^{-1/g}n^{2c} - 1 \geq c\mu^{-1}n^{c+1}.$$

For each m -tuple $X = (x_1, \dots, x_m) \in S^m$ and each integer $k \geq 3$, let $\gamma_k(X)$ be the number of sub- k -tuples of X that sum to zero. Let $\gamma(X) = \sum_{k=3}^{g-1} \gamma_k(X)$; that is, $\gamma(X)$ is the number of ‘ordered circuits’ of length less than g contained in X . Similarly, let $\zeta(X)$ denote the number of $(c - 1)$ -codimensional subspaces of $\text{GF}(2)^n$ that contain no element of X . Note that if $\gamma(X) = \zeta(X) = 0$, then the set Z of elements in X has critical number at least c and contains no small circuits, so

satisfies the lemma. We show with a probabilistic argument that the required m -tuple X exists.

Let $X = (x_1, \dots, x_m)$ be an m -tuple drawn uniformly at random from S^m . Since the last element in any k -tuple in S^k summing to zero is determined by the others, the probability that a k -tuple chosen uniformly at random from S^k sums to zero is at most $|S|^{-1}$, so we have $\mathbf{E}(\gamma_k(X)) \leq m^k |S|^{-1}$ for each k . By linearity, we have

$$\mathbf{E}(\gamma(X)) \leq |S|^{-1} \sum_{k=3}^{g-1} m^k < m^g |S|^{-1} \leq \frac{1}{2}.$$

We now consider $\zeta(X)$. Let F be an $(c-1)$ -codimensional subspace of $\text{GF}(2)^n$ and let W be a $(c-1) \times n$ binary matrix with null space F . If v is a vector chosen uniformly at random from S , then $v = v' + \mathbf{j}$, where \mathbf{j} is the all-ones vector and v' is chosen uniformly at random from S' , the set of vectors in $\text{GF}(2)^n$ of Hamming weight at most s . We have $v' + \mathbf{j} \in F$ if and only if $Wv' = W\mathbf{j}$. By Lemma 4.1, the probability that $Wv' = W\mathbf{j}$ is at least

$$\frac{1}{|S'|} \left(\frac{n}{2^c s} \right)^{s-c} \geq \left(\frac{s}{n} \right)^s \frac{n^{s-c}}{2^{c(s-c)} s^{s-c}} = \mu n^{-c}.$$

Therefore the probability that $x_i \notin F$ for all $i \in \{1, \dots, m\}$ is at most $(1 - \mu n^{-c})^m$; since there are at most $2^{(c-1)n}$ subspaces F of codimension $c-1$, it follows that

$$\mathbf{E}(\zeta(X)) \leq 2^{(c-1)n} (1 - \mu n^{-c})^m \leq 2^{(c-1)n} \left(2^{-\mu n^{-c}} \right)^m,$$

Now, using $m \geq c\mu^{-1}n^{c+1}$, we have $(c-1)n - m\mu n^{-c} \leq -n \leq -1$. Therefore $\mathbf{E}(\zeta(X)) \leq \frac{1}{2}$. This gives $\mathbf{E}(\gamma(X) + \zeta(X)) < 1$, so the required tuple X_0 with $\gamma(X_0) = \zeta(X_0) = 0$ exists. \square

5. CRITICAL THRESHOLDS

We now formulate a conjecture predicting the critical threshold for every simple binary matroid, and prove that this prediction is a correct lower bound. To state the conjecture, we use a piece of new terminology. If $k \geq 0$ is an integer and M is a simple rank- n binary matroid, viewed as a restriction of $G \cong \text{PG}(n-1, 2)$, then a k -codimensional subspace of M is a set of the form $F \cap E(M)$, where F is a rank- $(n-k)$ flat of G . Such a set is a flat of M and has rank at most $n-k$, but can also have smaller rank; for example, \emptyset is a 1-codimensional subspace of any simple binary matroid of critical number 1.

Let \mathcal{N} denote the class of simple binary matroids of critical number 2; we partition \mathcal{N} into three subclasses as follows:

- Let \mathcal{N}_0 denote the class of all $N \in \mathcal{N}$ having a 1-codimensional subspace S such that S is independent in N , and each odd circuit of N contains at least four elements of $E(N) - S$.
- Let $\mathcal{N}_{1/4}$ denote the class of all $N \in \mathcal{N} - \mathcal{N}_0$ so that some 1-codimensional subspace of N is independent in N .
- Let $\mathcal{N}_{1/2} = \mathcal{N} - (\mathcal{N}_0 \cup \mathcal{N}_{1/4})$.

We know from Corollary 1.5 that binary matroids of critical number 1 have critical threshold 0. Our first conjecture predicts the threshold for the binary matroids of critical number 2.

Conjecture 5.1. *For $\delta \in \{0, \frac{1}{4}, \frac{1}{2}\}$, each matroid in \mathcal{N}_δ has critical threshold δ .*

Note that every simple binary matroid N of critical number $c \geq 2$ has a $(c - 2)$ -codimensional subspace F such that $\chi(N|F) = 2$. Thus, the minimum in the following conjecture is well-defined, and the conjecture, which clearly implies Conjecture 1.7, predicts the critical threshold for every simple binary matroid of critical number at least 2.

Conjecture 5.2. *If N is a simple binary matroid of critical number $c \geq 2$, then the critical threshold for N is $1 - (1 - \delta)2^{2-c}$, where $\delta \in \{0, \frac{1}{4}, \frac{1}{2}\}$ is minimal such that $N|S \in \mathcal{N}_\delta$ for some $(c-2)$ -codimensional subspace S of N .*

Theorem 5.4 will show that the value given by the above conjecture is a correct lower bound for the critical threshold. The next lemma deals with the case when N has critical number 2.

Lemma 5.3. *Let $\delta \in \{0, \frac{1}{4}, \frac{1}{2}\}$. For all integers $c, r \geq 0$ and $\varepsilon > 0$, there is a simple binary matroid M of critical number at least c such that $|M| \geq (\delta - \varepsilon)2^{r(M)}$ and every restriction of M of rank at most r either has critical number at most 1, or is in $\mathcal{N}_{\delta'}$ for some $\delta' < \delta$.*

Proof. We consider the three values of δ separately. For $\delta = 0$, a matroid M given by Lemma 4.2 with critical number at least c and girth at least $r + 2$ will do, since every rank- r restriction of M is a free matroid and thus has critical number at most 1. For the other values of δ we require slightly more technical constructions.

Case 1: $\delta = \frac{1}{4}$. Let $g = r + 2$ and let $s = 2cg$. By Stirling's approximation we have $\binom{2n}{n} \sim \frac{1}{\sqrt{\pi n}} 2^{2n}$. Let $n \in \mathbb{N}$ be such that $\binom{2n}{n} \leq \frac{2\varepsilon}{gs} 2^{2n}$, and such that there exists a set $X \subseteq \text{GF}(2)^{2n}$, given by Lemma 4.2, for which $\text{wt}(x) \geq 2n - s$ for each $x \in X$, and $M(X)$ has rank $2n$, girth at least g , and critical number at least c . Let

$$Y = \{y \in \text{GF}(2)^{2n} : \text{wt}(y) \leq n - gs\}.$$

Let $X', Y' \subseteq \text{GF}(2)^{n+1}$ be defined by $X' = \left\{ \begin{bmatrix} 0 \\ x \end{bmatrix} : x \in X \right\}$ and $Y' = \left\{ \begin{bmatrix} 1 \\ y \end{bmatrix} : y \in Y \right\}$. Let $M = M(X' \cup Y')$. First note that $\chi(M) \geq \chi(M(X')) \geq c$. By symmetry of binomial coefficients and the fact that $\binom{2n}{i} \leq \binom{2n}{n}$ for each i , we have

$$|M| \geq |Y| \geq \sum_{i=0}^{n-gs} \binom{2n}{i} \geq \frac{1}{2} \left(2^{2n} - 2gs \binom{2n}{n} \right) \geq \left(\frac{1}{4} - \varepsilon \right) 2^{2n+1},$$

so $|M| \geq \left(\frac{1}{4} - \varepsilon \right) 2^{r(M)}$. Finally, let R be a restriction of M with $r(R) \leq r$. The set $E(R) \cap X'$ contains a 1-codimensional subspace S of R , and since $M(X') = M(X)$ has girth at least $g = r(R) + 2$, the set S is independent in R ; it follows that $\chi(R) \leq 2$. We argue that if $\chi(R) = 2$ then $R \in \mathcal{N}_0$.

Let C be an odd circuit of R with $|C - X'| \leq 2$, and let $C_X, C_Y \subseteq \text{GF}(2)^{2n}$ be the subsets of X and Y corresponding to $C \cap X'$ and $C \cap Y'$ respectively. Note that $\sum C_X = \sum C_Y$, and $|C_X| + |C_Y| \leq r(R) + 1 = g - 1$, with $|C_Y| \in \{0, 2\}$ and $|C_X|$ odd. By choice of Y we know that $\text{wt}(\sum C_Y) \leq 2(n - gs)$. Since every $x \in C_X$ has the form $\mathbf{j} + \hat{x}$ where \mathbf{j} is the all-ones vector and $\text{wt}(\hat{x}) \leq s$, we have $\text{wt}(\sum C_X) \geq 2n - (g - 1)s > 2(n - gs) \geq \text{wt}(\sum C_Y)$, a contradiction. Therefore each odd circuit of R contains at least four elements of $E(R) - S$, so $R \in \mathcal{N}_0$.

Case 2: $\delta = \frac{1}{2}$. Let $g = r + 2$ and n be an integer such that there is a set $X \subseteq \text{GF}(2)^n$, given by Lemma 4.2, so that $M(X)$ has girth at least g and critical number at least c . Let $X' = \left\{ \begin{bmatrix} 0 \\ x \end{bmatrix} : x \in X \right\}$ and let $Y' = \left\{ \begin{bmatrix} 1 \\ y \end{bmatrix} : y \in \text{GF}(2)^n \right\}$. Let $M = M(X' \cup Y')$.

Clearly $\chi(M) \geq \chi(M(X)) \geq c$ and $|M| \geq 2^n \geq \left(\frac{1}{2} - \varepsilon \right) 2^{r(M)}$. If R is a restriction of M with $r(R) \leq r$, then the set $E(R) \cap X'$ contains a 1-codimensional subspace S of R and, since $M(X')$ has girth at least $g \geq r(R) + 2$, the set S is independent in R . It follows that $\chi(R) \leq 2$ and $R \notin \mathcal{N}_{1/2}$. \square

We can now show that Conjecture 5.2 provides a valid lower bound.

Theorem 5.4. *If N is a simple rank- r binary matroid with critical number $c \geq 2$, then the critical threshold for N is at least $1 - (1 - \delta)2^{2-c}$, where $\delta \in \{0, \frac{1}{4}, \frac{1}{2}\}$ is minimal so that $N|S \in \mathcal{N}_\delta$ for some $(c - 2)$ -codimensional subspace S of N .*

Proof. Let $t \in \mathbb{Z}$ and let $\varepsilon > 0$. By Lemma 5.3 there exists a rank- n matroid M_0 for which $\chi(M_0) \geq t$ and $|M_0| \geq (\delta - \varepsilon)2^n$, and such that every restriction R_0 of M_0 with $r(R_0) \leq r$ satisfies either $\chi(R_0) \leq 1$ or $R_0 \in \mathcal{N}_{\delta'}$ for some $\delta' < \delta$. Let $G \cong \text{PG}(n + c - 3, 2)$ have M_0 as a restriction, and let $F_0 = \text{cl}_G(M_0)$. Set $M = G \setminus (F_0 - E(M_0))$.

Since M_0 is a restriction of M , we have $\chi(M) \geq t$. Moreover,

$$\begin{aligned} |M| &= |G| - |F_0| + |M_0| \\ &\geq (2^{n+c-2} - 1) - (2^n - 1) + (\delta - \varepsilon)2^n \\ &= (1 - (1 - \delta + \varepsilon)2^{2-c})2^{n+c-2} \\ &\geq (1 - (1 - \delta)2^{2-c} - \varepsilon)2^{r(M)}. \end{aligned}$$

Finally, suppose for a contradiction that M has a restriction $R \cong N$. The set $E(R) \cap F_0$ contains a $(c-2)$ -codimensional subspace S of R , and $\chi(R|S) \geq \chi(R) - (c-2) = 2$. However, $R|S$ is also a restriction of M_0 of rank at most r , so either $\chi(R|S) = 1$ or $R|S \in \mathcal{N}_{\delta'}$ for some $\delta' < \delta$. The former contradicts $\chi(R|S) \geq 2$ and the latter contradicts the minimality of δ . \square

Finally, we restate and prove Theorem 1.6.

Theorem 5.5. *If N is a simple binary matroid of critical number $c \geq 1$ so that $\chi(N \setminus I) = c$ for every rank- $(r(N) - c + 1)$ independent set I of N , then the critical threshold for N is $1 - 2^{1-c}$.*

Proof. The upper bound is given by Corollary 1.5, which also gives the theorem when $c = 1$. It thus suffices by Theorem 5.4 to show that N has no $(c-2)$ -codimensional subspace in $\mathcal{N}_0 \cup \mathcal{N}_{1/4}$. Indeed, if S is such a subspace then $N|S$ has an independent 1-codimensional subspace I , so $\chi((N|S) \setminus I) = 1$. Moreover, $r_N(I) \leq r_N(S) - 1 = r(N) - c + 1$, and $\chi(N \setminus I) \leq 1 + (c-2) < c$, a contradiction. \square

ACKNOWLEDGEMENTS

We thank the referees for their careful reading of the manuscript and for their useful comments.

REFERENCES

- [1] P. Allen, J. Böttcher, S. Griffiths, Y. Kohayakawa, R. Morris, The chromatic thresholds of graphs, *Adv. Math.* 235 (2013): 261–295.
- [2] J.E. Bonin, H. Qin, Size functions of subgeometry-closed classes of representable combinatorial geometries, *Discrete Math.* 224, (2000) 37–60.
- [3] S. Brandt, S. Thomassé, Dense triangle-free graphs are four-colorable, to appear, *JCTb*.
- [4] H.H. Crapo, G.-C. Rota, On the foundations of combinatorial theory: Combinatorial geometries, M.I.T. Press, Cambridge, Mass., 1970.

- [5] P. Erdős, Graph theory and probability, *Canad. J. Math.* 11 (1959) 34–38.
- [6] P. Erdős, M. Simonovits, On a valence problem in extremal graph theory, *Discrete Math.* 5 (1973), 323–334.
- [7] P. Erdős, A.H. Stone, On the structure of linear graphs, *Bull. Amer. Math. Soc.* 52, (1946) 1087–1091.
- [8] H. Furstenberg, Y. Katznelson, An ergodic Szemerédi theorem for IP-systems and combinatorial theory, *Journal d’Analyse Mathématique* 45, (1985) 117–168.
- [9] W. Goddard, J. Lyle, Dense graphs with small clique number, *J. Graph Theory* 66 (2011) no. 4, 319–331.
- [10] B. Green, Finite field models in additive combinatorics, *Surveys in combinatorics 2005*, London Mathematical Society Lecture Note Series 327 (Cambridge University Press, Cambridge, 2005), pp. 1–27.
- [11] B. Green, A Szemerédi-type regularity lemma in abelian groups, with applications, *Geometric & Functional Analysis GAFA* 15 (2005), 340–376.
- [12] J. Geelen, P. Nelson, An analogue of the Erdős-Stone theorem for finite geometries, *Combinatorica*, in press.
- [13] J. Geelen, P. Nelson, Odd circuits in dense binary matroids, *Combinatorica*, to appear.
- [14] R. Häggkvist, Odd cycles of specified length in nonbipartite graphs, *Graph theory* (Cambridge, 1981), 89–99.
- [15] F. Jaeger, A constructive approach to the critical problem for matroids, *Eur. J. Combin.* 2 (1981), 137–144.
- [16] T. Łuczak, S. Thomassé, Coloring dense graphs via VC-dimension, [arXiv:1007.1670 \[math.CO\]](https://arxiv.org/abs/1007.1670)
- [17] J. G. Oxley, *Matroid Theory*, Oxford University Press, New York (2011).
- [18] T. C. Tao, V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge (2006).
- [19] C. Thomassen, On the chromatic number of triangle-free graphs of large minimum degree, *Combinatorica* 22 (2002), 591–596
- [20] D.J.A. Welsh, *Matroid Theory*, Academic Press, London (1976). Reprinted 2010, Dover, Mineola.